State of West Virginia Office of Technology Policy:

# IT Policy and Procedure Development

*Issued by the CTO*



## 1.0 PURPOSE

This policy establishes the form and content criteria for the West Virginia Office of Technology (WVOT) regarding information technology (IT) policy and procedure development, maintenance, and distribution to agencies within the State of West Virginia Executive Branch.

## 2.0 SCOPE

This policy applies to all employees engaged in developing technology policies or procedures, unless classified as "exempt" in West Virginia Code Section 5A-6-8, "Exemptions." The State's users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Instant Messaging services.

*Target Audience: Management*.

## 3.0 RELEVANT DOCUMENTS

3.1 West Virginia Office of Technology (WVOT) Page

3.2 WVOT Policies Issued by the Chief Technology Officer (CTO).

3.3 West Virginia Code §5A-6-4a – "Duties of the Chief Technology Officer Relating to Security of Government Information"

## 4.0 POLICY

4.1 All State IT and Information Security policies and procedures must be periodically updated and made available, electronically and in a timely manner, to all individuals/agencies within the Executive Branch, to assure compliance with policy objectives and to establish the responsibility of those affected by each policy and procedure.

4.2 Agencies may establish more stringent IT policies; however, duplication of content should be avoided.

4.3 Each agency developing a security policy supplement **must** submit it to the WVOT for review.

4.4 The WVOT Policy Unit within the Office of Information Security and Controls (OISC) is responsible for developing and maintaining effective IT and Information Security policy and procedure. This Unit works closely with interested and affected individuals, technical editors, and subject matter experts, as needed.

4.4.1 The WVOT is responsible for establishing and coordinating IT policies and procedures. Final authority for WVOT policies falls to the CTO.

4.5 Every employee is responsible for abiding by all State IT policies and relevant procedures. Emergency Temporary Policy

4.6 Under certain conditions, the CTO may need to set emergency temporary policies, which will take effect immediately.

4.6.1 The emergency temporary policy will remain in effect for 180 calendar days from the date signed by the CTO. The date may be extended as necessary.

4.6.2 The WVOT will publish the emergency temporary policy and post it to the WVOT Internet policy page.

4.6.3 The emergency temporary policy is then subject to the usual procedure for adopting a permanent policy.

4.7 State employees may view all policies by accessing the WVOT Internet policy page at: go.wv.gov/wvotpolicies

4.8 Both State IT policies and procedures are defined by a set of criteria in order to provide consistency.

4.9 Agency management is responsible for communicating IT policies and procedures to all current State employees.

4.10 Each agency will designate an individual who will be responsible for reviewing all policies and procedures, if applicable, with all newly transferred and hired employees.

4.11 Any State employee may either request that a new IT policy or procedure be written, or propose that revisions to an existing document be made.

4.12 Maintaining Policies and Procedures

4.12.1 Policies and procedures related to information and data system security are reviewed annually, updated as needed, and approved by the relevant department, CISO, and then by the CTO.

4.12.2 The WVOT is responsible for posting and maintaining all IT policies on the State's policy web page: (www.technology.wv.gov). Procedures will be posted to the Intranet only.

4.12.3 To ensure consistency, the WVOT has created a standard format for both policies and procedures to facilitate the adoption of clear, concise documents at all levels of State agencies.

4.13 The WVOT will designate an individual(s) to review and amend (as needed) IT policies and procedures at least once every two years.

4.13.1 Substantive changes to policy or procedure may only be made with CTO approval.

4.13.2 When revisions to a policy or procedure are necessary, the CTO will determine whether the changes will require a global notification.

4.14 Approved policies and procedures remain in effect and are only replaced at the release of a new or modified document.

4.15 Any modified or temporary policy or procedure that materially affects the usage rights or responsibilities of employees will be communicated to agencies by a global e-mail message alert.

4.16 Each agency will be responsible for maintaining an IT policy manual in a central location for employees who do not have access to the Internet.

## 5.0 ENFORCEMENT & AUTHORITY

Under the provisions of West Virginia Code §5A-6-4a *et seq*., the Chief Technology Officer (CTO) is charged with securing State government information and the data communications infrastructure from unauthorized uses, intrusions, or other security threats. The CTO is granted both the authority and the responsibility to develop

information technology policy, promulgate that policy, audit for policy compliance, and require corrective action where compliance is found to be unsatisfactory or absent.

This policy is one in a series of IT-related policies intended to define and enable the incorporation of appropriate practices into all activities using State-provided technology in the State of West Virginia. To the extent that there are policies in place which provide less security than this policy, they will be superseded by this policy. In instances where existing state and federal laws and regulations are more restrictive than information security policies issued by the WVOT the more restrictive provisions will prevail.

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action will be administered by the employing agency and may be based upon recommendations of the WVOT and the West Virginia Division of Personnel.

Violations of this policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination. The State may also be required by law to report certain illegal activities to the proper law enforcement agencies.

## 6.0 DEFINITIONS

6.1 Chief Technology Officer (CTO) – The person responsible for the State's information resources.

6.2 Contractor/Subcontractor – Anyone who has a contract with the State or one of its entities.

6.3 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of Information Technology and Security policy, the term "employee" shall include the following: contractors, subcontractors, contractors' employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the WVOT to be subject to this policy. This definition does not create any additional rights or duties.

6.4 Information Security Administrator (ISA) – The person designated by the agency head to assure the agency's compliance with State Information Security policies and procedures. The ISA is the agency's internal and external point of contact for all Information Security matters.

6.5 IT Policy – Written statements defining requirements and compliance mandates in the conduct of employees of the State of West Virginia. Only the CTO may issue policy statements relating to IT.

6.6 Office of Information Security and Controls (OISC) - The functional unit charged with the responsibility to undertake and sustain initiatives to promote, enhance, monitor, and govern actions, standards, and activities necessary to safeguard data and information systems within the Executive Branch of WV, as provided in West Virginia Code §5A-6-4a and the Governor's Executive Order No. 6-06.

6.7 West Virginia Division of Personnel – A division of the Department of Administration established by West Virginia Code § 29-6-1 *et seq*., which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.

6.8 West Virginia Office of Technology (WVOT)- The division of the Department of Administration established by WV Code § 5A-6-4a, *et. seq.,* which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

6.9 WVOT Policy Unit - The Unit responsible for developing and maintaining IT and/or Information Security policy and procedure.